SN 10/588,608

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001084176 A**

(43) Date of publication of application: **30.03.01**

(51) Int. Cl **G06F 12/14**

(21) Application number: **11262299**

(22) Date of filing: **16.09.99**

(71) Applicant: **DENSO CORP**

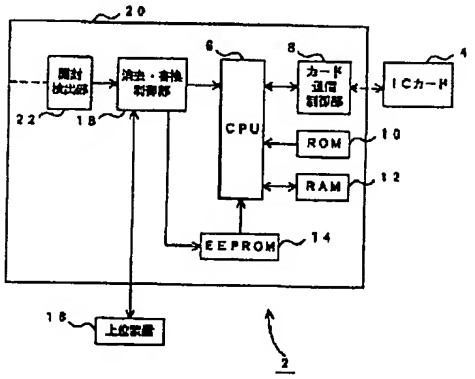
(72) Inventor: **TAKAHASHI KIYOSHI**

(54) **DEVICE AND METHOD FOR PREVENTING UNAUTHORIZED READING**

(57) Abstract:

PROBLEM TO BE SOLVED: To preserve security in an electronic controller in which a storing means for storing data or the like is arranged in a casing, and to prevent information from being lost when the casing is regularly opened.

SOLUTION: When it is detected that a casing is opened by an opening detecting part 22, the storage contents of an EEPROM 14 are deleted by a deleting and rewriting controlling part 18. Thus, the security can be preserved. Then, the contents stored in the EEPROM 14 are loaded from a host device 16 to the EEPROM 14 by the deleting and rewriting controlling part 18. In this unauthorized reading preventing method, a person who can restore the storage contents is limited to a person who has the host device 16, that is, a person who can regularly open a casing 20 of an IC card reader/writer 2. Thus, it is possible to prevent a person who tries to unauthorizedly read the storage contents from restoring the storage contents or reading the storage contents.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－84176
（P2001－84176A）
(43)公開日　平成13年３月30日(2001.3.30)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｄ　５Ｂ０１７

審査請求　未請求　請求項の数７　ＯＬ　（全６頁）

(21)出願番号　特願平11－262299

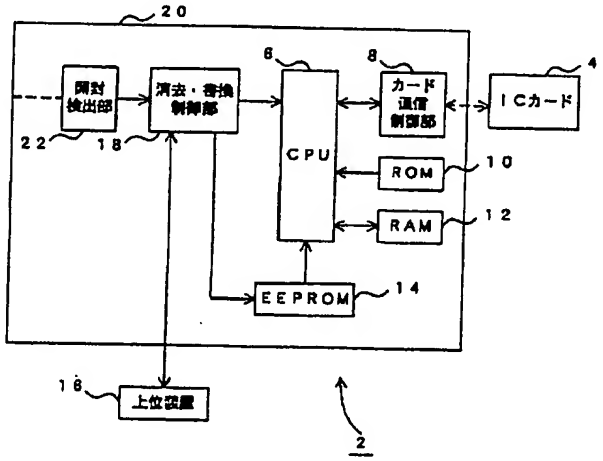
(22)出願日　平成11年９月16日(1999.9.16)

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(72)発明者　高橋　清志
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
(74)代理人　100082500
弁理士　足立　勉

Ｆターム(参考)　5B017 AA07 BA08 BB03 CA11

(54)【発明の名称】　不正読み出し防止装置およびその方法

(57)【要約】
【課題】　データ等を記憶した記憶手段を筐体内に備えた電子制御装置において、セキュリティを保ちつつ、正規に開封を行なった場合には、情報が失われないようにする。
【解決手段】　筐体が開封されたことが開封検出部２２によって検出されると、消去書換制御部１８がＥＥＰＲＯＭ１４の記憶内容を消去する。これによりセキュリティは保たれる。そして消去書換制御部１８が、ＥＥＰＲＯＭ１４に記憶されていた内容を上位装置１６からＥＥＰＲＯＭ１４にロードする。この不正読み取り防止方法によれば、記憶内容を復元できる者は上位装置１６を持っている者すなわち正規にＩＣカードリーダライタ２の筐体２０を開封する者に限られ、不正に記憶内容を読み出そうとする者は、記憶内容を復元することができず、従って記憶内容を読み出すことができない。



1

【特許請求の範囲】

【請求項１】　コンピュータプログラムおよびデータの少なくとも一方を記憶した記憶手段を筐体内に備えた電子制御装置に対し、前記記憶手段から記憶内容を不正に読み出す、という不正が行われるのを防止する不正読み出し防止装置であって、

前記筐体が開封されたことを検出する開封検出手段と、

該開封検出手段によって前記筐体が開封されたことが検出されると、前記記憶手段の記憶内容を消去する消去制御手段と、

該消去制御手段により前記記憶手段の記憶内容が消去された後に、該記憶内容を当該電子制御装置に接続された外部装置から前記記憶手段にロードする記憶内容復元手段と、

を備えたことを特徴とする不正読み出し防止装置。

【請求項２】　当該電子制御装置が、該コンピュータプログラムを実行するプログラム実行手段を備えたものであり、

前記開封検出手段により前記筐体の開封が検出されると前記プログラム実行手段を停止させる実行停止手段と、

前記記憶内容復元手段により前記記憶手段の記憶内容が復元されると前記プログラム実行手段を再起動する再起動手段とを備えたことを特徴とする請求項１に記載の不正読み出し防止装置。

【請求項３】　前記記憶内容復元手段が、

前記消去制御手段により前記記憶手段の記憶内容が消去された後、前記筐体が密閉されていることを検出する密閉検出手段と、

該密閉検出手段により、前記筐体が密閉されていることを検出されると、当該電子制御装置に接続された前記外部装置から前記記憶内容を前記記憶手段にロードする密閉時復元手段と、

を備えたものであることを特徴とする請求項１または２に記載の不正読み出し防止装置。

【請求項４】　前記記憶手段が、当該電子制御装置に設けられたバッテリーからの給電によって記憶内容がバックアップされる記憶素子であり、

前記消去制御手段が、前記筐体が開封されると前記バッテリーから前記記憶素子への給電経路を遮断するスイッチであることを特徴とする請求項１から３にいずれか記載の不正読み出し防止装置。

【請求項５】　コンピュータプログラムおよびデータの少なくとも一方を記憶した記憶手段を筐体内に備えた電子制御装置に対し、前記記憶手段から記憶内容を不正に読み出す、という不正行為を防止する不正読み出し防止方法であって、

前記筐体が開封されると前記記憶手段の記憶内容を消去し、該記憶内容を当該電子制御装置に接続された外部装置から前記記憶手段にロードすることを特徴とする不正読み出し防止方法。

2

【請求項６】　当該電子制御装置が、コンピュータプログラムを実行するプログラム実行手段を備えたものであり、

前記筐体の開封が検出されると前記プログラム実行手段を初期化し、前記記憶手段の記憶内容が復元されると前記プログラム実行手段を再起動することを特徴とする請求項５に記載の不正読み出し防止方法。

【請求項７】　前記記憶手段の記憶内容が消去された後、前記筐体が密閉されると、当該電子制御装置に接続された前記外部装置から前記記憶内容を前記記憶手段にロードすることを特徴とする請求項５または６に記載の不正読み出し防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータプログラムおよびデータの少なくとも一方を記憶した記憶手段を筐体内に備えた電子制御装置に対し、記憶手段から記憶内容が不正に読み出されるのを防止する技術に関する。

【０００２】

【従来の技術】近年、様々な製品が電子制御化されたり情報機器化されるに伴いこれらのセキュリティ性を高めたいというニーズが高まっている。このニーズに対応するため、情報の暗号化などを施し第３者には情報の内容は分からないようにしている。しかし悪意を持つものは製品内部の動作を解析し、暗号のアルゴリズムや鍵などの不正入手やプログラムの改変等を行なう可能性がある。このため製品の開封時には製品内の情報の消去や物理的に動作しなくなるような防御が既に行なわれている。例えば、ＩＣカードには、そのパッケージ（ここではこうしたものも含めて以下、筐体と呼ぶ）を開封すると、内部の電子回路が破壊されることにより、記憶内容の漏洩を防ぐものがある。

【０００３】

【発明が解決しようとする課題】しかしながら、上記従来技術によれば、正規のメンテナンスや正規の故障解析時にも電子回路が破壊されてしまうので、開封前の状態に戻せないという問題があった。

【０００４】本発明はかかる課題に鑑みなされたもので、請求項１に記載の不正読み出し防止装置および請求項５に記載の不正読み出し防止方法は、セキュリティを保ちつつ、正規に開封を行なった場合にも情報が失われないようにすることを目的としている。

【０００５】また請求項２に記載の不正読み出し防止装置および請求項６に記載の不正読み出し防止方法は、筐体に内蔵されたＣＰＵなどの動作解析が行なわれないようにすることを目的としている。また更に、請求項３に記載の不正読み出し防止装置および請求項７に記載の不正読み出し防止方法は、セキュリティを一層高めることを目的としている。

【０００６】そして請求項４に記載の不正読み出し防止装置は、消去制御手段を簡素に実現する態様を提示するものである。

【０００７】

【課題を解決するための手段及び発明の効果】かかる課題を解決するためになされた本発明の請求項１に記載の不正読み出し防止装置は、筐体が開封されたことが開封検出手段によって検出されると、消去制御手段が記憶手段の記憶内容を消去する。ここで記憶手段には、コンピュータプログラムおよびデータの少なくとも一方が記憶されている。すなわち、これら双方が記憶されていても良いし、これらの内の一方に加え、その他のものが記憶されていても良い。これによりセキュリティは保たれる。ただしこれでは正規に開封を行なった場合にも記憶手段の記憶内容が失われてしまうので、記憶内容復元手段が、記憶手段に記憶されていた内容を当該電子制御装置に接続された外部装置から記憶手段にロードする。

【０００８】当然のことながら外部装置には、記憶手段の記憶内容が予め記憶されている。そもそも記憶手段の記憶内容は秘密扱いであるから、少なくともこれを記憶している状態の外部装置の存在も秘密扱いになる。従って、記憶内容を復元できる者はこれらの者に限られ、不正に記憶内容を読み出そうとする者は、記憶内容を復元することができず、従って記憶内容を読み出すことができない。

【０００９】従って、請求項１に記載の不正読み出し防止装置によれば、セキュリティを保ちながらも、正規に開封を行なった場合には記憶内容を復元することができるので情報が失われない。なお、外部装置には常時、記憶手段の記憶内容が保持されていても良いし、正規のメンテナンスや解析を行なう者の携行するフロッピーディスク、ＲＯＭなどの記録媒体に前記記憶内容を記録しておき、これをメンテナンス時に外部装置に読み取らせてもよい。

【００１０】また請求項２に記載の不正読み出し防止装置では、筐体の開封が検出されると実行停止手段が、筐体に内蔵されたプログラム実行手段（ＣＰＵなどのマイクロプロセッサが代表的）を停止させる。そして記憶内容復元手段により記憶手段の記憶内容が復元されると、再起動手段がプログラム実行手段を再起動する。

【００１１】従って、請求項２に記載の不正読み出し防止装置によれば、プログラム実行手段の動作解析が行なわれるのを防止することができる。なお、プログラム実行手段によって実行されるプログラムは、記憶手段に記憶させたものでもよいし、当該電子制御装置の外にある装置（前記外部装置に限らない）が記憶しているプログラムでも良い。

【００１２】請求項３に記載の不正読み出し防止装置では、記憶手段の記憶内容が消去された後、筐体が密閉されていることが密閉検出手段によって検出されると、密閉時復元手段が外部装置から記憶内容を記憶手段にロードする。これに反し、筐体の密閉を確認することなく、外部装置から記憶内容を記憶手段にロードすると、開封された筐体内に不正行為をする者が取り付けた機器などにより、ロード後に記憶内容が読み出される虞がある。

【００１３】この点、請求項３に記載の不正読み出し防止装置によれば、こうした行為を防止できるのでセキュリティを一層高めることができる。請求項４に記載の不正読み出し防止装置においては、記憶手段を、当該電子制御装置に設けられたバッテリーからの給電によって記憶内容がバックアップされる記憶素子（例えばＳＲＡＭ（Static Random Access Memory））とし、消去制御手段を、筐体が開封されるとバッテリーから記憶素子への給電経路を遮断するスイッチとしている。

【００１４】こうすれば、筐体が開封されたときには着実に記憶素子の内容が失われる、という作動を、スイッチとバッテリーと記憶素子とを主要構成として実現でき、特に消去制御手段として複雑な処理をする必要が一切ない。従って、請求項４に記載の不正読み出し防止装置によれば、消去制御手段を簡素に実現することができる。

【００１５】なお、請求項１、２、３の不正読み出し防止装置を不正読み出し防止方法として構成したのが、それぞれ請求項５、６、７に記載の本発明であり、それぞれ対応する不正読み出し防止装置と同様の効果を奏することができる。

【００１６】

【発明の実施の形態】以下に本発明の実施の形態の一例を図面と共に説明する。まず、図１は本発明のを適用したＩＣカードリーダライタ２の概略を示すブロック図である。ＩＣカードリーダライタ２は、ＩＣカード４に対してカードデータの読み出し及び書き込みを行なう装置である。

【００１７】ＩＣカードリーダライタ２は、ＣＰＵ６と、ＩＣカード４との通信を制御するカード通信制御部８と、ＣＰＵ６が実行するコンピュータプログラム（以下、単にプログラムという）を記憶したＲＯＭ１０と、ＣＰＵ６がプログラムを実行する際のデータを一時的に記憶するＲＡＭ１２と、ＣＰＵ６が実行するプログラムの内、特に秘匿性の高いプログラム（例：暗号化のアルゴリズム）やデータ（例：暗号化や解読に用いる鍵）を保持すると共に必要に応じてこれら記憶内容を消去可能なＥＥＰＲＯＭ１４と、各種ロジック回路から構成され、ＥＥＰＲＯＭ１４のデータの消去を行なったりＩＣカードリーダライタ２に接続された上位装置１６からデータを受け取ったりする消去書換制御部１８と、ＩＣカードリーダライタ２の筐体２０が開放されているか閉じられているかを検出する赤外線スイッチを備えた開封検出部２２とを備えている。また上位装置１６には、ＥＥＰＲＯＭ１４に記憶されている内容と同じものが予め記

5

憶されているものとする。

【００１８】ＣＰＵ６は、ＲＯＭ１０に記憶されているプログラムを実行し、適宜ＥＥＰＲＯＭ１４に格納されているデータを用いたり実行の作業領域としてＲＡＭ１２を使用したりすることによりＩＣカード４に対するデータの読み取りや書き込みを行なう。一方、消去書換制御部１８は、筐体２０が開放・密閉に応じて前述の作動をすると共に、ＣＰＵ６の動作の停止及び起動の指令を発する。この消去書換制御部１８の行なう処理を図２に示す。

【００１９】図２は、消去書換制御部１８によって実行される不正読み出し防止処理のフローチャートである。本処理は、筐体２０が開放されたことが開封検出部２２によって検出されると開始される。本処理が開始されるとまずＳ１０にてＣＰＵ６の動作を停止させ、Ｓ２０にてＥＥＰＲＯＭ１４の記憶内容を消去する。そしてＳ３０にて筐体２０が閉じているか否かを開封検出部２２の検出結果に基づいて判定する。閉じていない場合は筐体２０が閉じられるまで待機する。筐体２０が閉じられるとＳ４０に移行し、上位装置１６が当該ＩＣカードリーダライタ２に接続されているか否かを判定する。接続されていなければ本処理を終了する。接続されていれば、Ｓ５０に進み、プログラムおよびデータを上位装置１６からダウンロードする。ダウンロードされたプログラムやデータは一旦、図示しないバッファに保持され、Ｓ６０にてＥＥＰＲＯＭ１４に格納されていく。続くＳ７０ではダウンロードが正常終了したか否かを判定し、終了していなければＳ５０に戻る。ダウンロードが正常終了していれば、Ｓ８０に進みＣＰＵ６を起動し、本処理を終了する。

【００２０】以上のような処理を行なう消去書換制御部１８を備えたＩＣカードリーダライタ２によれば、筐体２０を開封するとＥＥＰＲＯＭ１４の内容がＳ２０の処理によって消去されるため、セキュリティが保たれる。また、正規のメンテナンスや解析においては、上位装置１６をＩＣカードリーダライタ２に接続して筐体２０を閉じれば、Ｓ３０～Ｓ７０の処理によりＥＥＰＲＯＭ１４の内容が復元されるので、情報が失われない。なお、これと同様のことを、不正にＥＥＰＲＯＭ１４の記憶内容を読み出そうとする者が行なってＥＥＰＲＯＭ１４の内容の復元を試みようにも、上位装置１６が存在しないため不可能である。また、Ｓ１０、Ｓ８０の処理により、筐体２０が開けられている間はＣＰＵ６が停止されるため、ＣＰＵ６の動作が解析されることもない。

【００２１】ここで、本実施の形態の構成と本発明の必須要件との対応関係を示す。ＥＥＰＲＯＭ１４が記憶手段に相当し、開封検出部２２が開封検出手段および密閉検出手段に相当し、ＣＰＵ６がプログラム実行手段に相

6

当し、上位装置１６が外部装置に相当し、不正読み出し防止処理のＳ１０が実行停止手段に相当し、同処理のＳ２０が消去制御手段に相当し、同処理のＳ３０、Ｓ５０～Ｓ６０が密閉時復元手段に相当し、同処理のＳ８０が再起動手段に相当し、ＩＣカードリーダライタ２が電子制御装置に相当する。

【００２２】以上、本発明を適用した実施の形態の一例として、ＩＣカードリーダライタ２について説明してきたが、本発明はこうした実施例に何等限定されるものではなく様々な態様で実施しうる。例えば、このような不正読み出し防止方法をＩＣカードリーダライタ２以外の電子機器に適用しても良い。

【００２３】また、開封検出部２２として赤外線スイッチを用いたが、それ以外の物理スイッチ（例えば、リミットスイッチ）を用いても良い。プログラム実行手段に相当するものとしてＣＰＵ６を使用したが、その他の電子素子（例えば、ＦＰＧＡ）を用いても良い。また、消去書換制御部１８を実現するに際し、ＣＰＵ６とは別途、ＣＰＵを設け、これに不正読み出し防止処理に相当する処理を実行させても良い。

【００２４】また記憶手段に相当するものとしてＥＥＰＲＯＭ１４を用いたが、その他のメモリ（例えば、フラッシュメモリ、強誘電体メモリ、ＳＲＡＭ）にしてもよい。特にＳＲＡＭの場合には、ＳＲＡＭのバックアップをするバッテリや電池からＳＲＡＭまで電力を供給する経路が筐体２０を開放すると遮断されるように構成しておくと、不正読み出し防止処理の起動およびＳ２０の動作を極めて簡素に実現することができる。また、消去書換制御部１８の動作電源と記憶手段の電源とを共有にしておけば、消去書換制御部１８が動作不能時に記憶手段の内容も消去されるため、更にセキュリティが向上する。

【００２５】また前述の不正読み出し防止処理では、Ｓ３０で筐体２０が閉じていることを確認していたが、上位装置１６がない限りＳ５０のダウンロードが不可能であるため、Ｓ３０は省略しても良い。

【図面の簡単な説明】

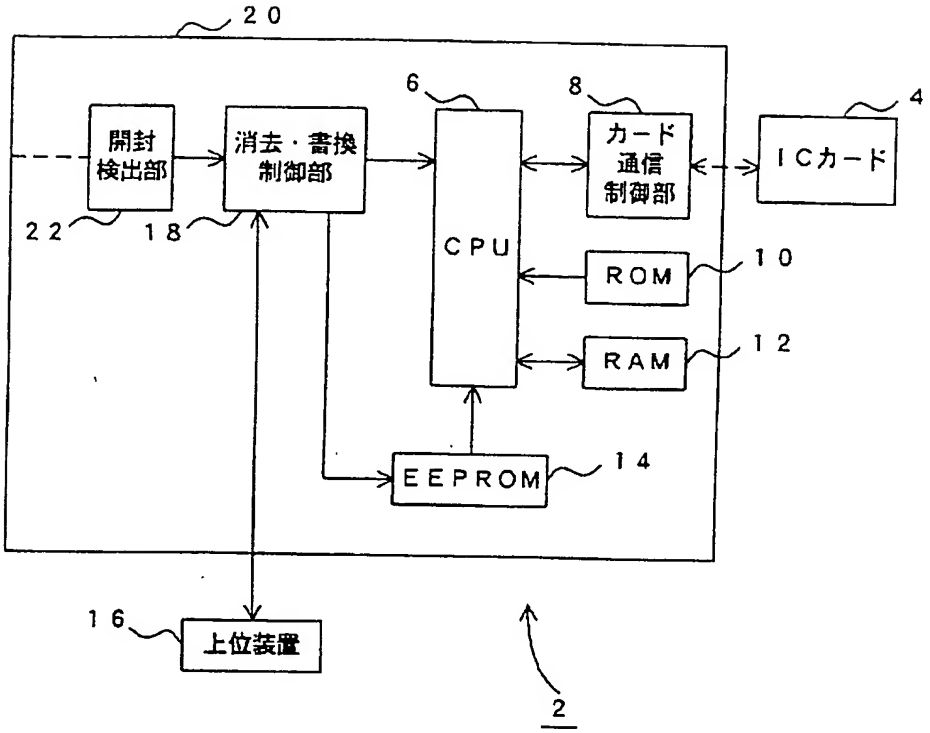
【図１】　本発明を適用したＩＣカードリーダライタ２のブロック図である。

【図２】　ＩＣカードリーダライタ２の消去書換制御部１８が実行する不正読み出し防止処理のフローチャートである。

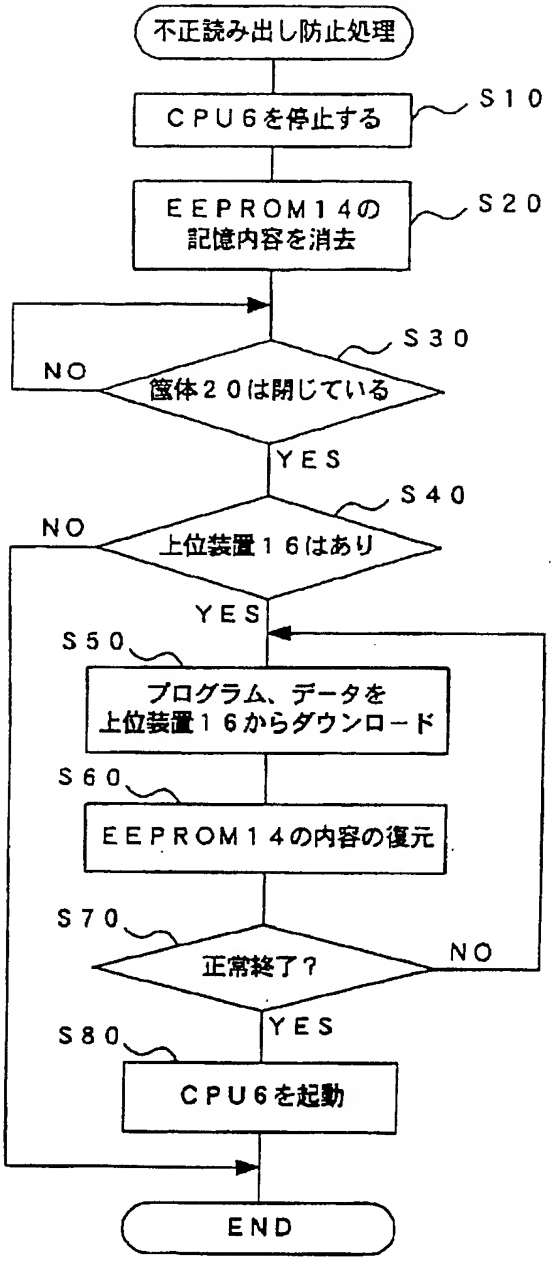
【符号の説明】

２…ＩＣカードリーダライタ
４…ＩＣカード　　６…ＣＰＵ
８…カード通信制御部　１４…ＥＥＰＲＯＭ
１６…上位装置　　１８…消去書換制御部
２０…筐体　　２２…開封検出部

【図１】


２０
６
８
４
開封
検出部
消去・書換
制御部
カード
通信
制御部
ＩＣカード
２２
１８
ＣＰＵ
ＲＯＭ
１０
ＲＡＭ
１２
ＥＥＰＲＯＭ
１４
１６
上位装置
２

【図２】


不正読み出し防止処理
ＣＰＵ６を停止する
Ｓ１０
ＥＥＰＲＯＭ１４の
記憶内容を消去
Ｓ２０
Ｓ３０
ＮＯ
筐体２０は閉じている
ＹＥＳ
Ｓ４０
ＮＯ
上位装置１６はあり
ＹＥＳ
Ｓ５０
プログラム、データを
上位装置１６からダウンロード
Ｓ６０
ＥＥＰＲＯＭ１４の内容の復元
Ｓ７０
正常終了？
ＮＯ
ＹＥＳ
Ｓ８０
ＣＰＵ６を起動
ＥＮＤ